

# ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 31 PAGES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 07/26/2017		2. CONTRACT NO. (if any) HSBP1017A00024		6. SHIP TO:	
3. ORDER NO.		4. REQUISITION/REFERENCE NO. 0020097724		a. NAME OF CONSIGNEE See Attached Delivery Schedule	
5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229				b. STREET ADDRESS	
				c. CITY	d. STATE
				e. ZIP CODE	
				f. SHIP VIA	
7. TO:				8. TYPE OF ORDER	
a. NAME OF CONTRACTOR MCKINSEY COMPANY INC WASHINGTON DC				<input checked="" type="checkbox"/> a. PURCHASE -- Reference Your . Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
b. COMPANY NAME				<input type="checkbox"/> b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
c. STREET ADDRESS 1200 19TH ST NW STE 1100				10. REQUISITIONING OFFICE (b) (6), (b) (7) (C)	
d. CITY WASHINGTON		e. STATE DC	f. ZIP CODE 20036-2412		
9. ACCOUNTING AND APPROPRIATION DATA N/A					
11. BUSINESS CLASSIFICATION (Check appropriate box(es))					12. F.O.B. POINT
<input type="checkbox"/> a. SMALL <input checked="" type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)					Destination
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 07/25/2018	16. DISCOUNT TERMS Within 30 days Due net
a. INSPECTION	b. ACCEPTANCE				
DESTINATION	DESTINATION				

## 17. SCHEDULE ( See reverse for Rejections )

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Accpt
10	Integrated Consulting Services BPA	1.000	AU			

SEE BILLING INSTRUCTIONS REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		17(h)TOT (Cont. pages)
	21. MAIL INVOICE TO:				
	a. NAME DHS - Customs & Border Protection Commercial Accounts Sect.				17(i) GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) 6650 Telecom Drive, Suite 100				
	c. CITY Indianapolis	d. STATE IN	e. ZIP CODE 46278		

22. UNITED STATES OF AMERICA BY (Signature) 

(b) (6), (b) (7)(C)

ACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPR  
Previous edition not usable

OPTIONAL FORM 347 (REV. 2/2012)

Prescribed by GSA/FAR 48 CFR 53.213 (f)

DATE OF ORDER 07/26/2017	CONTRACT NO. (if any) HSBP1017A00024	ORDER NO.	PAGE OF PAGES 2 31
-----------------------------	---	-----------	-----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP. Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.**

**NOTES:**

BLANKET PURCHASE AGREEMENT (BPA) INTEGRATED CONSULTING SERVICES (ICS) UNDER THE PROFESSIONAL SERVICES SCHEDULE (PSS)

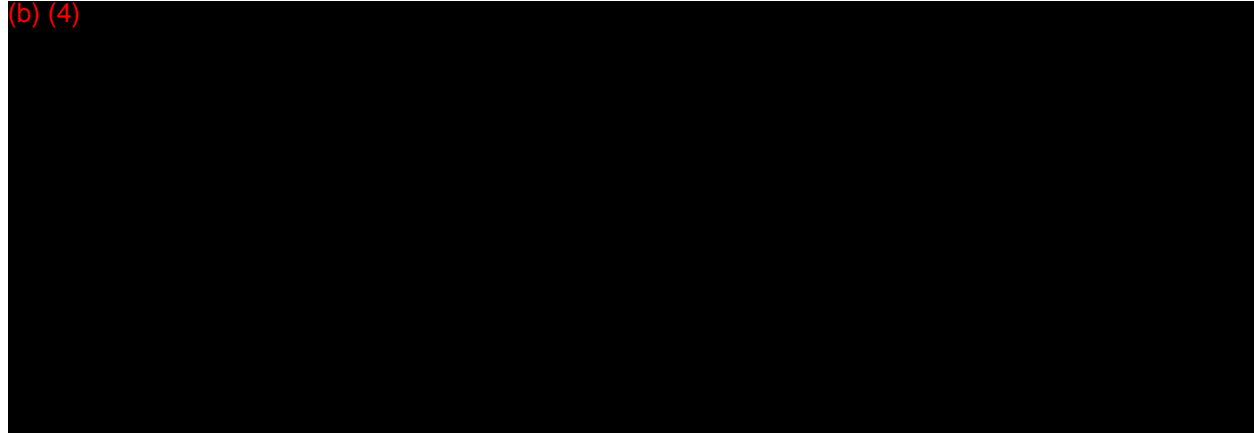
In accordance with the Federal Acquisition Streamlining Act, the United States (U.S) Customs and Border Protection (CBP) is establishing a multiple awardee Blanket Purchase Agreement (BPA) utilizing the General Service Administration (GSA) Professional Services Schedule (PSS) 00CORP contract for Integrated Consulting Services. This is a multiple awardee BPA to McKinsey & Company, Inc. Washington D.C. Altogether, the ICS BPA's will have a combined not-to-exceed (NTE) ceiling value of [REDACTED]. The BPA will allow for a task order type of either Firm-Fixed-Price (FFP) or Labor Hour (LH). The BPA Statement of Work (SOW) provided in the solicitation is hereby incorporated by reference. This BPA outlines and provides for specific pricing, clauses and other terms and conditions, beyond what is set forth in the GSA PSS Schedule.

The BPA consists of a one-year base period and four (4) one-year option periods. The BPA Periods are as follows:

Base Period:	July 26, 2017 through July 25, 2018
Option Period 1:	July 26, 2018 through July 25, 2019
Option Period 2:	July 26, 2019 through July 25, 2020
Option Period 3:	July 26, 2020 through July 25, 2021
Option Period 4:	July 26, 2021 through July 25, 2022

**SECTION I – BPA PRICING SCHEDULE**

**I.1 BPA PRICING\***



\*Weekly Rate

**I.2 LABOR CATEGORY DESCRIPTIONS AND MINIMUM QUALIFICATIONS**

Labor Category / Team Type	Team Description	Personnel Category, Education and Experience
Team A (EM+1)	<p><u><b>Team A integrates seven distinctive capabilities into a seamless offering:</b></u></p> <ul style="list-style-type: none"><li>● <b>Committed leadership by two McKinsey Partners/Senior Partners (part-time)</b>, who are accountable for delivery, actively manage the engagement, and lead problem solving with the team.</li><li>● <b>A full-time team of one Engagement Manager and one Associate or Business Analyst</b>, who lead the day-to-day work (e.g., interviews and data collection, analysis, problem solving, communications). The full-time team draws upon the following resources, capabilities, and expertise as much as needed to deliver superior results to the client.</li><li>● <b>Content experts (part-time)</b>, who bring world-class expertise and experience on relevant industry and functional topics.</li><li>● <b>Proprietary knowledge and tools</b> that help our clients solve problems more efficiently and effectively.</li><li>● Support for <b>new solutions and advanced analytic techniques</b>.</li><li>● A <b>research team</b> that is available around-the-clock to answer clients' questions about issues such as best practices or important trends.</li><li>● World-class <b>graphics support</b>.</li></ul>	See "Team Personnel" Table Below

<b>Team B (EM+2)</b>	<b><u>Team B integrates seven distinctive capabilities into a seamless offering:</u></b> <ul style="list-style-type: none"><li>● Committed leadership by two McKinsey Partners/Senior Partners (part-time), who are accountable for delivery, actively manage the engagement, and lead problem solving with the team.</li><li>● A full-time team of one Engagement Manager and two Associates or Business Analysts, who lead the day-to-day work (e.g., interviews and data collection, analysis, problem solving, communications). The full-time team draws upon the following resources, capabilities, and expertise as much as needed to deliver superior results to the client.</li><li>● Content experts (part-time), who bring world-class expertise and experience on relevant industry and functional topics.</li><li>● Proprietary knowledge and tools that help our clients solve problems more efficiently and effectively.</li><li>● Support for new solutions and advanced analytic techniques.</li><li>● A research team that is available around-the-clock to answer clients' questions about issues such as best practices or important trends.</li><li>● World-class graphics support.</li></ul>	See "Team Personnel" Table Below
<b>Team C (EM+3)</b>	<b><u>Team C integrates seven distinctive capabilities into a seamless offering:</u></b> <ul style="list-style-type: none"><li>● Committed leadership by at least two and sometimes three McKinsey Partners/Senior Partners (part-time), who are accountable for delivery, actively manage the engagement, and lead problem solving with the team.</li><li>● A full-time team of one Engagement Manager and three Associates or Business Analysts, who lead the day-to-day work (e.g., interviews and data collection, analysis, problem solving, communications). The full-time team draws upon the following resources, capabilities, and expertise as much as needed to deliver superior results to the client.</li><li>● Content experts (part-time), who bring world-class expertise and experience on relevant industry and functional topics.</li><li>● Proprietary knowledge and tools that help our clients solve problems more efficiently and effectively.</li><li>● Support for new solutions and advanced analytic techniques.</li><li>● A research team that is available around-the-clock to answer clients' questions about issues such as best practices or important trends.</li><li>● World-class graphics support.</li></ul>	See "Team Personnel" Table Below
<b>Team D (EM+4)</b>	<b><u>Team D integrates seven distinctive capabilities into a seamless offering:</u></b> <ul style="list-style-type: none"><li>● Committed leadership by at least two and sometimes three McKinsey Partners/Senior Partners (part-time), who are accountable for delivery, actively manage the engagement, and lead problem solving with the team.</li><li>● A full-time team of one Engagement Manager and four Associates or Business Analysts, who lead the day-to-day work (e.g., interviews and data collection, analysis, problem solving, communications). The full-time team draws upon the following resources, capabilities, and expertise as much as needed to deliver superior results to the client.</li><li>● Content experts (part-time), who bring world-class expertise and experience on relevant industry and functional topics.</li><li>● Proprietary knowledge and tools that help our clients solve problems more efficiently and effectively.</li><li>● Support for new solutions and advanced analytic techniques.</li><li>● A research team that is available around-the-clock to answer clients' questions about issues such as best practices or important trends.</li><li>● World-class graphics support.</li></ul>	See "Team Personnel" Table Below



<b>Team E - (1 Asc)</b>	<p><b><u>Team E integrates seven distinctive capabilities into a seamless offering:</u></b></p> <ul style="list-style-type: none"> <li>● Committed <b>leadership by one McKinsey Partner (part-time)</b>, who is accountable for delivery, actively manages the engagement, and leads problem solving with the team.</li> <li>● A <b>full-time team of one Associate or Business Analyst</b>, who leads the day-to-day work (e.g., interviews and data collection, analysis, problem solving, communications). The full-time Associate or Business Analyst draws upon the following resources, capabilities, and expertise as much as needed to deliver superior results to the client.</li> <li>● <b>Content experts (part-time)</b>, who bring world-class expertise and experience on relevant industry and functional topics.</li> <li>● <b>Proprietary knowledge and tools</b> that help our clients solve problems more efficiently and effectively.</li> <li>● Support for <b>new solutions and advanced analytic techniques</b>.</li> <li>● A <b>research team</b> that is available around-the-clock to answer clients' questions about issues such as best practices or important trends.</li> <li>● World-class <b>graphics support</b>.</li> </ul>	See "Team Personnel" Table Below
<b>Leadership Counseling</b>	<p><b><u>Leadership counseling integrates five distinctive capabilities into a seamless offering:</u></b></p> <ul style="list-style-type: none"> <li>● Committed <b>leadership by one McKinsey Partner (part-time)</b>, who is accountable for delivery and actively manages the engagement.</li> <li>● <b>Content experts (part-time)</b>, who bring world-class expertise and experience on relevant industry and functional topics.</li> <li>● <b>Proprietary knowledge and tools</b> that help our clients solve problems more efficiently and effectively.</li> <li>● Support for <b>new solutions and advanced analytic techniques</b>.</li> <li>● A <b>research team</b> that is available around-the-clock to answer clients' questions about issues such as best practices or important trends.</li> </ul>	See "Team Personnel" Table Below
<b>Management Workshop</b>	<p><b><u>Management workshop includes:</u></b></p> <ul style="list-style-type: none"> <li>● A Management Workshop is a <b>one-day event led by two consultants</b>, who meet with a group of clients to help them address a top management issue, understand industry trends, or build their skills. The consultants prepare materials, such as data analysis, interview summaries, market intelligence, best practices, and management options, to help ensure that the workshop is content-rich and fact-based. A Management Workshop includes a minimum of 4 and a maximum of 40 clients.</li> </ul>	See "Team Personnel" Table Below

Team Personnel

<b>Personnel Category</b>	<b>Education</b>	<b>Experience</b>
Senior Partner	Most Senior Partners have a graduate degree from a leading academic institution. At a minimum, Senior Partners have a Bachelor's degree.	<ul style="list-style-type: none"> <li>• Senior Partners typically have 20+ years of experience.</li> <li>• At a minimum, Senior Partners have 10 years of experience.</li> </ul>
Partner	Most Partners have a graduate degree from a leading academic institution. At a minimum, Partners have a Bachelor's degree.	<ul style="list-style-type: none"> <li>• Partners typically have 9-15 years of experience.</li> <li>• At a minimum, Partners have 5 years of experience.</li> </ul>

Engagement Manager	Most Engagement Managers have a graduate degree from a leading academic institution. At a minimum, Engagement Managers have a Bachelor's degree.	<ul style="list-style-type: none"><li>• Engagement Managers typically have 5-7 years of experience.</li><li>• At a minimum, Engagement Managers have 2 years of experience.</li></ul>
Associate	Most Associates have a graduate degree from a leading academic institution. At a minimum, Associates have a Bachelor's degree.	<ul style="list-style-type: none"><li>• Associates typically have 3-5 years of experience.</li><li>• At a minimum, Associates have 1 year of experience.</li></ul>
Business Analyst	At a minimum, Business Analysts have a Bachelor's degree.	<ul style="list-style-type: none"><li>• Business Analysts typically have 0-2 years of experience.</li><li>• At a minimum, Business Analysts have 0 years of experience and are recent college graduates.</li></ul>

## SECTION II – BPA TERMS AND CONDITIONS

The GSA Schedule 874 1 terms, conditions, and clauses are applicable to the awarded BPA. This BPA incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the BPA Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

<http://acquisition.gov/comp/far/index.html> or for DHS specific clauses at <http://farsite.hill.af.mil/VFHSARA.htm>.

### II.1 FAR/HSAR CLAUSES INCORPORATED BY REFERENCE

The following Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR) clauses are hereby added to the BPA. In the event that any of these clauses conflict with the GSA Federal Supply Schedule contract, the Federal Supply Schedule shall take precedence.

FAR 52.204-14	SERVICE CONTRACT REPORTING REQUIREMENTS (OCT 2016)
FAR 52.227-16	ADDITIONAL DATA REQUIREMENTS (JUNE 1987)
FAR 52.227-17	RIGHTS IN DATA – SPECIAL WORKS (DEC 2007)
HSAR 3052.203-70	INSTRUCTIONS FOR CONTRACTOR DISCLOSURE OF VIOLATIONS (JUN 2006)
HSAR 3052.205-70	ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASE (SEP 2012)

HSAR 3052.242-72 CONTRACTING OFFICER'S TECHNICAL  
REPRESENTATIVE (DEC 2003)

## II.2 FAR/HSAR CLAUSES INCORPORATED BY FULL TEXT

### **FAR 52.217-9 Option to Extend the Terms of the Contract (MAR 2000)**

(a) The Government may extend the term of this contract (each task order) by written notice to the Contractor within fifteen (15) days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least fifteen (15) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

(End of Clause)

### **HSAR 3052.204-71 Contractor Employee Access (SEP 2012)**

(a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, in-subordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of Clause)

#### **HSAR 3052.209-70 PROHIBITIONS ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006)**

##### **(a) Prohibitions.**

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

##### **(b) Definitions. As used in this clause:**

*Expanded Affiliated Group* means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting 'more than 50 percent' for 'at least 80 percent' each place it appears.

*Foreign Incorporated Entity* means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

*Inverted Domestic Corporation.* A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

- (2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—
- (i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or
- (ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and
- (3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

*Person, domestic, and foreign* have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

- (i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or
- (ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan deemed in certain cases.* If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain transfers disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships.* For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395 (b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

- (i) warrants;
- (ii) options;
- (iii) contracts to acquire stock;
- (iv) convertible debt instruments; and
- (v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

☐ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

☐ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

☐ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of Clause)

**HSAR 3052.215-70 Key Personnel of Facilities (DEC 2003)**

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under the BPA are as follows:

*Program Manager – To be determined at Task Order Level*

The Key Personnel or Facilities under the BPA Orders must be identified in each BPA Order.

(End of Clause)

**CONTRACT CLAUSE G.5, ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)**

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

- Invoices, including Certified Time Sheet for labor hour allocation for each task, Certified Materials Cost, Travel Cost details
- Proof of acceptance

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

**ADDITIONAL INVOICE INSTRUCTIONS FOR T&M ORDERS**

All T&M invoices shall comply with FAR 52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts, which requires adequate substantiation of all time and material costs.

(End of clause)

**SPECIAL CONTRACT CLAUSE H.40, SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)**

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- (3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- (4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(a) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

- (1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL



USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

- (2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
- (3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
- (4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.
- (b) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.
  - (1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.
    - (i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.
    - (ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies

as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

- (iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

- (5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include

disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

- (6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(c) Sensitive Information Incident Reporting Requirements.

- (1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.
- (2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:
- (i) Data Universal Numbering System (DUNS);
  - (ii) Contract numbers affected unless all contracts by the company are affected;
  - (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
  - (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
  - (v) Contracting Officer POC (address, telephone, email);
  - (vi) Contract clearance level;
  - (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
  - (viii) Government programs, platforms or systems involved;
  - (ix) Location(s) of incident;
  - (x) Date and time the incident was discovered;
  - (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
  - (xii) Description of the Government PII and/or SPII contained within the system;
  - (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
  - (xiv) Any additional information relevant to the incident.

(d) Sensitive Information Incident Response Requirements.

- (1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
- (2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
- (3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
  - (i) Inspections,
  - (ii) Investigations,
  - (iii) Forensic reviews, and
  - (iv) Data analyses and processing.
- (4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.
- (e) Additional PII and/or SPII Notification Requirements.
  - (1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.
  - (2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:
    - (i) A brief description of the incident;
    - (ii) A description of the types of PII and SPII involved;
    - (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
    - (iv) Steps individuals may take to protect themselves;
    - (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
    - (vi) Information identifying who individuals may contact for additional information.
- (f) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:
  - (1) Provide notification to affected individuals as described above; and/or
  - (2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

- (i) Triple credit bureau monitoring;
  - (ii) Daily customer service;
  - (iii) Alerts provided to the individual for changes and fraud; and
  - (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
- (3) Establish a dedicated call center. Call center services shall include:
- (i) A dedicated telephone number to contact customer service within a fixed period;
  - (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
  - (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
  - (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
  - (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
  - (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.
- (g) Certification of Sanitization of Government and Government-Activity-Related Files and Information.  
As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

Note 1: Applicability of an ATO will be required at time of Task Order Award. The activities which require an ATO will be discussed at time of issuance for each task order. More information will be given at task order level. Any and all information will be required to be stored on CBP's network. The activities which require an ATO will be discussed at time of issuance for each task order. More information will be given at task order level.

(End of clause)

**SPECIAL CONTRACT CLAUSE H.41, INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)**

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

**PRICING PROVISIONS FOR TASK ORDER OR BLANKET PURCHASE AGREEMENT ISSUED UNDER A FEDERAL SUPPLY SCHEDULE (JUN 2005)**

"This task order/Blanket Purchase Agreement (BPA) is placed under the terms and conditions of the GSA Federal Supply Schedule contract identified herein. The contractor warrants that, throughout performance, the prices charged the Government shall be as low as, or lower than, those charged the contractor's most favored customers and that the Government shall never be charged more under this order than the offeror/contractor's current GSA schedule rates, or the rates contained in the task order schedule, whichever are lower.

If this order contains options for additional periods of performance, U.S. Customs & Border Protection (CBP) will invoke the option only if the offeror/contractor maintains a current GSA schedule. Unilateral options will not be invoked if the rates indicated in the task order schedule for the option are higher than current GSA schedule rates, but may be invoked bilaterally at the offeror/contractor's current GSA rates. The contractor shall provide notice to the Government of any proposed and/or approved change to the GSA schedule rates. Failure to comply with the provisions of this price warranty may be cause for termination of the order and the offeror/contractor may be required to adjust their billing and/or reimburse the Government for any charges invoiced in violation of the price warranty."

(End of clause)

**CONTRACTING OFFICER'S AUTHORITY (MAR 2003)**

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or

condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

The following Primary Contracting Officer is assigned to this contract. Alternate Contracting Officers may be assigned:

Base BPA Contracting Officer:

NAME:  
PHONE NUMBER:  
EMAIL:

(b) (6), (b) (7)(C)

BPA Task Order Contracting Officer:

NAME: To be determined on individual BPA Orders

(End of clause)

#### CONTRACTING OFFICER'S REPRESENTATIVE (COR) AND TECHNICAL MONITORS

1. The principle role of the COR is to support the Contracting Officer in managing the contract. This is done through furnishing technical direction within the confines of the contract, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contracting Officer. As a team the Contracting Officer and COR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the Technical Monitor (TM) is to support the COR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

2. The Contracting Officer hereby designates the individual(s) named below as the Contracting Officer's Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

Base BPA CORs:

NAME:  
PHONE NUMBER:  
EMAIL:

(b) (6), (b) (7)(C)

BPA Task Order CORs:

NAME:  
PHONE NUMBER:  
EMAIL:

To be determined on individual BPA Orders

3. The COR(s) and TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COR, will be promptly provided to the Contractor by the Contracting Officer in writing.

4. The responsibilities and limitations of the COR are as follows:

- The COR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.

- The COR may designate assistant COR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
- The COR will maintain communications with the Contractor and the Contracting Officer. The COR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
- The COR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
- The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract's price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.
- The COR is not authorized to direct the Contractor on how to perform the work.
- The COR is not authorized to issue stop-work orders. The COR may recommend the authorization by the Contracting Officer to issue a stop work order, but the Contracting Officer is the only official authorized to issue such order.
- The COR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

5. The responsibilities and limitations of the TM are as follows:

- Coordinating with the COR on all work orders, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.
- Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding.
- Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COR for consideration.
- Informing the COR if the Contractor is not meeting performance, cost, schedule milestones.
- Performing technical reviews of the Contractor's proposals as directed by the COR.
- Performing acceptance of the Contractor's deliverables as directed by the COR.
- Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements.

#### **GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)**

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

(End of clause)

#### **DISCLOSURE OF INFORMATION (MAR 2003)**

##### **A. General**

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract.



B. Technical Data Rights

The Contractor shall not use, disclose, reproduce, or otherwise divulge or transfuse to any persons any technical information or data licensed for use by the Government that bears any type of restrictive or proprietary legend except as may be necessary in the performance of the contract. Refer to the Rights in Data clause for additional information.

C. Privacy Act

In performance of this contract the Contractor assumes the responsibility for protection of the confidentiality of all Government records and/or protected data provided for performance under the contract and shall ensure that (a) all work performed by any subcontractor is subject to the disclosure restrictions set forth above and (b) all subcontract work be performed under the supervision of the Contractor or their employees.

(End of clause)

**NON-PERSONAL SERVICE (MAR 2003)**

1. The Government and the contractor agree and understand the services to be performed under this contract are non-personal in nature. The Contractor shall not perform any inherently Governmental functions under this contract as described in Office of Federal Procurement Policy Letter 92-1

2. The services to be performed under this contract do not require the Contractor or his employees to exercise personal judgment and discretion on behalf of the Government, but rather, the Contractor's employees will act and exercise personal judgment and discretion on behalf of the Contractor.

3. The parties also recognize and agree that no employer-employee relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees. Contractor personnel under this contract shall not:

- (a) Be placed in a position where there is an appearance that they are employed by the Government or are under the supervision, direction, or evaluation of any Government employee. All individual employee assignments any daily work direction shall be given by the applicable employee supervisor.
- (b) Hold him or herself out to be a Government employee, agent or representative or state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as such and specify the name of the company of which they work.
- (c) Be placed in a position of command, supervision, administration or control over Government personnel or personnel of other Government contractors, or become a part of the government organization. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to change the contract in any way. If the other Contractor believes this communication to be direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.

4. If the Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the Contractor shall promptly notify the CO of this communication or action.

5. Rules, regulations directives and requirements which are issued by U.S. Customs & Border Protection under their responsibility for good order, administration and security are applicable to all personnel who enter U.S. Customs &

Border Protection installations or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

(End of clause)

#### **POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2014)**

##### **A. Contractor Performance Evaluations**

Interim and final performance evaluation reports will be prepared on this contract or order in accordance with FAR Subpart 42.15. A final performance evaluation report will be prepared at the time the work under this contract or order is completed. In addition to the final performance evaluation report, an interim performance evaluation report will be prepared annually to coincide with the anniversary date of the contract or order.

Interim and final performance evaluation reports will be provided to the contractor via the Contractor Performance Assessment Reporting System (CPARS) after completion of the evaluation. The CPARS Assessing Official Representatives (AORs) will provide input for interim and final contractor performance evaluations. The AORs may be Contracting Officer's Representatives (CORs), project managers, and/or contract specialists. The CPARS Assessing Officials (AOs) are the contracting officers (CO) or contract specialists (CS) who will sign the evaluation report and forward it to the contractor representative via CPARS for comments.

The contractor representative is responsible for reviewing and commenting on proposed ratings and remarks for all evaluations forwarded by the AO. After review, the contractor representative will return the evaluation to the AO via CPARS.

The contractor representative will be given up to fourteen (14) days to submit written comments or a rebuttal statement. Within the first seven (7) calendar days of the comment period, the contractor representative may request a meeting with the AO to discuss the evaluation report. The AO may complete the evaluation without the contractor representative's comments if none are provided within the fourteen (14) day comment period. Any disagreement between the AO/CO and the contractor representative regarding the performance evaluation report will be referred to the Reviewing Official (RO) within the division/branch the AO is assigned. Once the RO completes the review, the evaluation is considered complete and the decision is final.

Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file and may be used in future award decisions.

##### **A. Designated Contractor Representative**

The contractor must identify a primary representative for this contract and provide the full name, title, phone number, email address, and business address to the CO within 30 days after award.

##### **B. Electronic Access to Contractor Performance Evaluations**

The AO will request CPARS user access for the contractor by forwarding the contractor's primary and alternate representatives' information to the CPARS Focal Point (FP).

The FP is responsible for CPARS access authorizations for Government and contractor personnel. The FP will set up the user accounts and will create system access to CPARS.

The CPARS application will send an automatic notification to users when CPARS access is granted. In addition, contractor representatives will receive an automated email from CPARS when an evaluation report has been completed.

(End of clause)

#### **ADDITIONAL CONTRACTOR PERSONNEL REQUIREMENTS (OCT 2007)**

The Contractor will ensure that its employees will identify themselves as employees of their respective company while working on U.S. Customs & Border Protection (CBP) contracts. For example, contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.

(End of clause)

#### **SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)**

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).

b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self-certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.

c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self-certification, by public records check, or other reference checks conducted in the normal course of business.

2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: Logical Access means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

(End of clause)

#### **TRAVEL AND PER DIEM**

BPA Holder travel may be required to support the requirements of the BPA TO. Travel required by the Government outside the local commuting area(s) will be reimbursed to the BPA Holder in accordance with the Federal Travel Regulations (FTR). The BPA Holder shall be responsible for obtaining written approval from the BPA TO COR (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

The Government will not reimburse local travel within a 50-mile radius from the BPA Holder's primary place of performance. BPA Holder personnel may be required to travel to support the requirements of this contract and as stated on the delivery order. Travel performed for personal convenience or daily travel to and from work at the BPA

Holder's facility or local Government facility (i.e., designated work site) shall not be reimbursed hereunder. Local parking in the Washington, D.C. metropolitan area is not covered by this SOW.

Allowable travel costs will be reimbursed, if incurred and approved by the COR prior to departure, for the cost of transportation, lodging, subsistence and incidental expenses in accordance with the FTR. The BPA Holder shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes, and cancellations under nonrefundable airline tickets are reimbursable as long as the changes are driven by the work requirement. Long distance travel may be required both in the Contiguous United States (CONUS) and Outside the Contiguous United States (OCONUS). The BPA Holder shall coordinate specific travel arrangements with the COR to obtain advance, written approval for the travel about to be conducted. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs.

## **CONTRACTOR RESPONSIBILITY, CONDUCT, AND PERFORMANCE UNDER CBP SERVICE CONTRACTS**

### **A. BASIC REQUIRED STANDARDS OF CONDUCT RELATED TO BUSINESS UNDER GOVERNMENT CONTRACTS**

1. General. The Government has the basic inherent expectations of timely, focused, effective, and competent performance by the Contractor under a contract. The Contractor has the basic inherent expectation of fair treatment under the contract, where the Contractor's employees, when in Government facilities or in circumstances where the Government has primary control or responsibility, have the expectation of performance in a safe and non-hostile work environment.

2. Adherence to Standards. The Contractor shall adhere to the same professional and ethical standards of conduct required by the FAR and all other applicable laws and regulations. Contractor employees performing work under this contract shall not:

- a) Solicit new business (on-site at government spaces, or while on work during periods paid by Government) while performing work under the contract;
- b) Conduct business other than that which is covered by this contract during periods paid by the Government;
- c) Conduct business not directly related to this contract while on Government premises;
- d) Use Government computer systems or networks, Government property or materials, and/or Government facilities for company or personal business;
- e) Recruit while on Government premises or otherwise act to disrupt official Government business while on Government premises.
- f) Discuss with unauthorized persons any information obtained during the performance of work under this contract.

### **3. Reporting Matters.**

- a) Illegal and Unethical Conduct. The Contractor, and its employees shall immediately report to the Contracting Officer and/or Contracting Officer's Representative, any illegal or unethical conduct observed, noticed, or discovered while on Government premises or during periods paid by the Government under this contract, without regard as to the source of such conduct (except that any matter involving only contractor employees, apart from any Government requirements or the specific requirements of this contract, is deemed to be strictly the concern of the Contractor). The Contractor shall immediately report to the Government all actual or suspected violations of Government information, personnel, or physical security requirements. The Contractor shall fully comply with all of the reporting requirements that are expressed for specified circumstances and issues identified in discrete Federal Acquisition Regulation or Homeland Security Acquisition Regulation clauses in force under this contract.
- b) Emergency Situations While on Government Premises. Contractor employees shall immediately report any emergency situations they may witness (any circumstance where actual or potential loss of life, serious injury, or critical damage to property, or other serious incidents, such as fires, or workplace violence, terrorist activities, or other criminal behavior is occurring ) per standing CBP procedures while they are performing under contract in government facilities.

c) Government Employee Misconduct. In the event of misconduct by a government employee which is observed or witnessed by a contractor employee, (or in the event of any unauthorized conduct to which a Government employee may subject a contractor employee) the contractor employee shall immediately report such to their on-site contractor supervisor or other company-designated management official, the Contracting Officer and/or Contracting Officer's Representative.

d) Workplace safety. In the event of any situation involving workplace safety, the contractor employee shall immediately report such to their on-site contractor supervisor or other company -designated management official, the Contracting Officer and/or Contracting Officer's Representative.

4. The Contracting Officer may require dismissal from work under this contract and/or removal of access to government facilities, property, information and/or information systems of those employees which the Contracting Officer deems contrary to the public interest or inconsistent with the best interest of national security.

5. Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Sensitive But Unclassified, Government procurement sensitive information, and/or other sensitive information, or proprietary business information from other Contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contracting Officer will provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant.

#### B. BASIC REQUIREMENTS AFFECTING CONTRACTOR PERFORMANCE

1. Contractor Responsibility for Performance Management. The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.

2. Limitation on Government Liability. The Government shall not be liable for any injury to the Contractor's personnel or damage to the Contractor's property unless such injury or damage is due to negligence on the part of the Government and is recoverable under the Federal Torts Claims Act, or pursuant to another Federal statutory authority.

3. Responsibility for Effective Contract Transitions. A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition.

4. The Government observes the following holidays:

New Year's Day  
Martin Luther King, Jr. Birthday  
Washington's Birthday (President's Day)  
Memorial Day  
Independence Day  
Labor Day  
Columbus Day  
Veteran's Day  
Thanksgiving Day  
Christmas Day

a) In addition to the days designated as holidays, the Government observes also the following days:

- Any other day designated by Federal Statute, and
- Any other day designated by Executive Order, and
- Any other day designated by President's Proclamation, such as extreme weather conditions.
- Inauguration Day (Washington, DC metropolitan area)

b) When the Government grants excused absence to its employees in a specific location, assigned Contractor personnel at that same location may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Representative. Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract.

c) In the event the Contractor's personnel work during the holiday or other excused absences, they may be compensated by the Contractor, however, no form of holiday or other premium compensation will be considered either as a direct or indirect cost, other than their normal compensation for the time worked. For cost reimbursable and time and material (T&M) contracts, the Government will only consider as direct and/or indirect costs those efforts actually performed during the holiday or excused absences in the event contractor personnel are not dismissed. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

Otherwise, the management responsibility for contractor functions approved by the Contracting Officer for offsite work, in the event of inaccessibility of federal workplaces are the sole responsibility of the contractor. The contractor may propose telework or other solutions when critical work is required, however, the Contractor is solely responsible for any cost differential in performance, all liabilities that may be due to performance at an alternate location and all resources necessary to complete such performance.

d) In the event of an actual emergency, the Contracting Officer may direct the contractor to change work hours or locations or institute telework, utilize personal protective equipment or other mandated items.

C. CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES. If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property. The Contractor is responsible for maintaining all assigned space(s) in a clean and orderly fashion during the course of this contract. All telephones are for conducting official Government business only.

D. CONTRACTOR EMPLOYEE TRAINING REQUIREMENTS. The Contracting Officer's Representative will identify any specified government training which the contractor's employees with access to CBP IT accounts will be required to complete as a precursor to or coincident with their authorized access to or use of government space or facilities, equipment, information, or information systems as a necessary component of performance required under the contract. Contractor employees are responsible for providing required evidence of timely training completion when the Government assigns such training. The contractor shall provide fully trained and experienced personnel. Training of contractor personnel shall be performed by the contractor at its expense, except as directed by the Government through written authorization by the Contracting Officer to meet special requirements peculiar to the contract. Training includes attendance at seminars, symposia or user group conferences. Training will not be authorized for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art or for training contractor employees on equipment, computer languages and computer operating systems that are available on the commercial market or required by a contract. This includes training to obtain or increase proficiency in word processing, spreadsheets, presentations, and electronic mail.

E. COOPERATION WITH AUDITORS AND INVESTIGATORS. The Contractor shall cooperate fully with all auditors and investigators on all matters arising under or directly related to this contract and/or any other matter that may occur in relation to the contractor's presence within Government facilities or due to access to Government information, information systems, property or equipment.

F. EMPLOYEE REMOVAL. The Government may identify to the Contractor any contractor employee for removal from contract performance upon notification of failure to comply with the requirements herein.

G. EMPLOYEE TERMINATION. The contractor shall notify the Contracting Officer and the Contracting Officer's Representative within 48 hours when an employee performing work under this contract who has been granted access to government information, information systems, property, or government facilities access terminates employment, no longer is assigned to the contract, or no longer requires such access. The contractor shall be responsible for returning, or ensuring that employees return, all DHS/CBP -issued contractor/employee identification, all other CBP or DHS property, and any security access cards to Government offices issued by a landlord of commercial space.

H. PERSONNEL CHANGES. The Contractor shall notify the Contracting Officer's Representative (COR) in writing of any changes needed in building, information systems, or other information access requirements for its employees in order to meet contract requirements not later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other Contractors. The Contractor shall provide the following information to the COR: full name, social security number, effective date, and reason for change.

I. SUBSTITUTION OF KEY PERSONNEL. The Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Representative (COR) prior to making any changes in Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced or otherwise meet the standards applicable in the contract. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or forty-five (45) days if either a background investigation for building or information system access and/or a security clearance (due to classified contract requirements that relate specifically to personnel) must be obtained to meet the contract's requirements, in advance of the proposed substitution. Such notification from the contractor shall include:

1. an explanation of the circumstances necessitating the substitution;
2. a complete resume of the proposed substitute; and
3. any other information requested by the CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and COR will evaluate substitution requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

## **FLOW DOWN CLAUSES**

All applicable GSA Schedule contract clauses shall flow down to the awarded BPA and its BPA Task Orders. If the current GSA Schedule is replaced with a subsequent schedule, the applicable terms and conditions of the subsequent schedule shall be incorporated into this agreement and the term of such subsequent schedule shall also apply. However, a follow-on GSA Schedule will not impact the maximum term of the BPAs and its orders. Further, BPA pricing will only be impacted as a result of a bilateral modification to the BPAs.

## **BPA TERM**

The BPA consists of a one-year base period and four (4) one-year option periods. The BPA Periods are as follows:

Base Period: July 26, 2017 through July 25, 2018  
Option Period 1: July 26, 2018 through July 25, 2019  
Option Period 2: July 26, 2019 through July 25, 2020  
Option Period 3: July 26, 2020 through July 25, 2021  
Option Period 4: July 26, 2021 through July 25, 2022

The BPA shall remain in effect for a maximum of one year from the date of award. This BPA includes four (4) one-year option periods that may be exercised in accordance with FAR 52.217-9. Individual order periods of performance shall be specified in each BPA Task Order. BPA Task Orders may be issued at any time during the BPA period of performance.

Periods of Performance for BPA Task Orders for services issued in the final year of the BPA shall not extend beyond one year after the BPA's ordering period end date. The period of performance for each BPA Task Order shall be consistent with the funding appropriation being obligated.

If the BPA Holder fails to perform in a manner satisfactory to the CO, this BPA may be canceled with 30 days written notice to the BPA Holder by the CO.

#### **CONTRACT TYPE (OCT 2008)**

The multiple award BPA includes fixed labor rates to be used for integrated consulting services procured under BPA Task Orders. Orders placed against this BPA may be Firm-Fixed Price (FFP) or Labor Hour (LH). No profit shall be applied by the Contractor in support of ODCs.

#### **ORDER OF PRECEDENCE**

All orders placed against the BPA are subject to the terms and conditions of the contractor's GSA schedule contract. In the event of any inconsistencies between the provisions of the order, the BPAs and the GSA Schedule, the provisions of the Schedule contract will take precedence.

#### **OBLIGATION**

This BPA does not obligate any funds. Funds will be obligated by the placement of task orders.

#### **BPA VOLUME**

The Government estimates, but does not guarantee, that the volume of purchases for ICS BPA holders will be approximately a combined \$40 million over five (5) years. The Government is obligated only to the extent of authorized purchases actually made under the BPA.

There is no minimum order guarantee.

#### **AUTHORIZED USERS**

The only office authorized to issue task orders under this BPA is the U.S. Customs and Border Protection, Office of Acquisitions, Procurement Directorate.

#### **ORDER ADMINISTRATION**

BPA Task Orders and their administration will be accomplished by a duly appointed CO assigned by CBP.

#### **ORDERING PROCEDURES**

All work to be ordered under this BPA will be through BPA Task Orders. The following ordering procedures apply to all BPA Task Orders:

- Ordering procedures shall be in accordance with FAR 8.405-3(c)(2). Task order solicitations will be issued to all BPA awardees.
- All funding will be provided via the BPA Task Order. A BPA Task Order will be considered issued when the CO transmits a funded BPA Task Order to the contractor.
- All costs associated with preparation and/or discussion of the Contractor's order quotations will be at the Contractor's expense.
- The BPA Task Order shall include a requirements statement in the form of a Statement of Work (SOW), Statement of Objectives (SOO), or Performance Work Statement (PWS) which will describe the specific work requirements and objectives; the deliverables that will be required; the period of performance of the work; reporting requirements;



performance measures and expectations; and any other special requirements (including travel) necessary to perform the work.

- Place of performance shall be specified on each individual BPA order (See Section III.8 of the Statement of Work).
- Organizational Conflict of Interest (OCI) Risk Mitigation Plans will be required from BPA holders. If you do not submit an OCI Risk Mitigation Plan, you will be required to explicitly state your reasons to the Contracting Officer. If any such conflict of interest is found to exist, the Contracting Officer may disqualify the offeror. Please see HSAR 3052.209-72 Organizational Conflict of Interest (JUN 2006) for further instructions.

#### **ANNUAL REVIEW OF THE BPA**

In accordance with FAR Subpart 8.405-3(e), the BPA will be reviewed annually to:

1. Ensure that authorized procedures are being followed;
2. Determine whether current circumstances warrant continuation of the BPA;
3. Determine that the BPA still represents the best value to the Government;
4. Ensure the GSA Schedule contract is still in effect; and,
5. Determine whether estimated annual amounts have been exceeded.

Exceeding the estimated volume amounts may warrant additional consideration or price reductions by the awardee to DHS.

#### **TERMINATION**

Notwithstanding any other provision relating to this BPA and BPA Task Orders issued thereunder, the Ordering CO may terminate any BPA Task Order under the BPA at any time in accordance with the termination provisions contained in FAR Subpart 8.406-4 *Termination for Cause* or FAR Subpart 8.406-5 *Termination for Convenience*.

#### **SECURITY REQUIREMENTS**

Any security requirements beyond those required in this BPA shall be specified in each BPA Task Order whether included in full text or by reference.

#### **BPA ORDER CLOSEOUT**

It is the intention of the Government to perform close-out procedures on an individual BPA Order basis. The Contractor agrees to perform those internal functions necessary to support the close-out process in a timely manner. BPA Order close-out will generally occur as soon as possible after completion of the work involved.

#### **SOLICITATION PROVISIONS INCORPORATED BY REFERENCE**

FAR 52.217-5	EVALUATION OF OPTIONS (JULY 1990)
FAR 52.250-2	SAFETY ACT COVERAGE NOT APPLICABLE (FEB 2009)

#### **SOLICITATION PROVISIONS INCORPORATED BY FULL TEXT**

##### **FAR 52.216-31 Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition (Feb 2007)**

- (a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
- (b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
  - (1) The offeror;
  - (2) Subcontractors; and/or

(3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

(End of Provision)

**HSAR 3052.209-72 Organizational Conflict of Interest (JUN 2006)**

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting is based on the information and knowledge gained in performance of task orders awarded under the BPA. Potentially, the task orders for the CBP Commissioner, Deputy Commissioner, and Agency Leadership Council may influence the direction of future agency policy giving unfair advantage to future agency-wide requirements. Contractors would be performing tasks, either as the Prime or as Sub-contractors, on functions including management or strategy consulting, including research, change management, communication plans, evaluations, studies, analyses, scenarios/simulations, reports, business policy and regulation development assistance, strategy formulation on issues related to organization, operations, and business technology, facilitation and related decision support services, survey services, using a variety of methodologies, including survey planning, design, and development; survey administration; data validation and analysis; reporting, and stakeholder briefings, advisory and assistance services in accordance with FAR 37.203, mission-oriented business projects or programs and the achievement of mission performance goals.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

\_\_\_ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

\_\_\_ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divisions that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of Provision)

**HSAR 3052.209-73 LIMITATION OF FUTURE CONTRACTING (JUN 2006)**

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict is: *(1) When either the contractor, core team member(s) and/or subcontractor has access to procurement sensitive information that may provide it an unfair advantage in competing for some or all of the proposed effort, (2) contractor's performance of work which may affect the outcome of other work (perform analysis and evaluation and exercise subjective judgement; designing and implanting of own products; development of some specifications will determine future use to make uses of those specifications), (3) the contractor reviews the work of itself or any affiliates; and (4) offers advice or planning in areas in which the contractor or any affiliates have financial interests tied to particular solutions.*

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

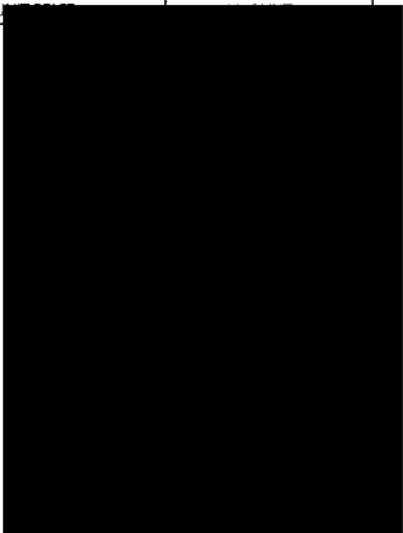
(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of Clause)

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS</b>				1. REQUISITION NUMBER 0020105171		PAGE OF PAGES 1 3	
<b>OFFEROR TO COMPLETE BLOCKS 12,17,23,24, &amp; 30</b>							
2. CONTRACT NO. HSBP1017A00024		3. AWARD/EFF. DATE 07/16/2018		4. ORDER NUMBER 70B01C18F00000497		5. SOLICITATION NUMBER	
6. SOLICITATION ISSUE DATE		7. FOR SOLICITATION INFORMATION CALL:		a. NAME [REDACTED]		b. TELEPHONE NUMBER (No collect calls) [REDACTED]	
8. OFFER DUE DATE/ LOCAL TIME		9. ISSUED BY CODE 7014  DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229		10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR:  <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> EDWOSB NAICS: 541611 SIZE STANDARD: \$15.0 MILLION <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A)			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input checked="" type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS Within 30 days Due net		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)  13b. RATING		14. METHOD OF SOLICITATION <input checked="" type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP	
15. DELIVER TO CODE  See Attached Delivery Schedule				16. ADMINISTERED BY CODE  DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229			
17a. CONTRACTOR/ CODE OFFEROR 825229318 FACILITY CODE  MCKINSEY COMPANY INC WASHINGTON DC  1200 19TH ST NW STE 1100  WASHINGTON DC 20036-2412  TELEPHONE NO.				18a. PAYMENT WILL BE MADE BY CODE  DHS - Customs & Border Protection Commercial Accounts Sect.  6650 Telecom Drive, Suite 100 Indianapolis IN 46278			
17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER.				18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. <input type="checkbox"/> SEE ADDENDUM			
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
20	Contract Support Services			1.000	AU	[REDACTED]	
30	Contract Support Services			1.000	AU		
40	Contract Support Services			1.000	AU		
50	Contract Support Services			1.000	AU		
60	Contract Support Services			1.000	AU		
70	Contract Support Services			1.000	AU		
80	Contract Support Services			1.000	AU		
25. ACCOUNTING AND APPROPRIATION DATA PLEASE SEE ATTACHMENT						26. TOTAL AWARD AMOUNT (For Govt Use Only) [REDACTED]	
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.							
<input checked="" type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED ADDENDA <input type="checkbox"/> ARE <input checked="" type="checkbox"/> ARE NOT ATTACHED.							
<input type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.				<input checked="" type="checkbox"/> 29. AWARD OF CONTRACT: REF. 06/13/2018 OFFER DATED YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:			
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) [REDACTED]			
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER [REDACTED]		31c. DATE SIGNED	

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS</b>		1. REQUISITION NUMBER 0020105171	PAGE OF PAGES 2 3
Continuation Sheet			

2. CONTRACT NO. HSBP1017A00024	3. AWARD/EFF. DATE 07/16/2018	5. SOLICITATION NUMBER
-----------------------------------	----------------------------------	------------------------

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. U	24.
90	Contract Support Services	1.000	AU		
100	Contract Support Services	1.000	AU		
110	Contract Support Services	1.000	AU		
120	Contract Support Services	1.000	AU		
130	Contract Support Services	1.000	AU		
140	Contract Support Services	1.000	AU		
150	Contract Support Services	1.000	AU		
160	Contract Support Services	1.000	AU		
170	Contract Support Services	1.000	AU		
180	Contract Support Services	1.000	AU		
190	Contract Support Services	1.000	AU		

CONTRACT NO.:  
HSBP1017A00024REQUISITION NUMBER  
0020105171AWARD/EFF. DATE  
07/16/2018

## ADDITIONAL INFORMATION:

The purpose of task order 01C18F0497, via BPA HSBP1017A00024, is to award U.S. Customs and Border Protection's (CBP) Strategy Plan requirement to McKinsey & Company, Inc. Washington D. C.

The period of performance is for July 16, 2018 to July 15, 2019. Task order is funded at a firm-fixed-price (FFP) total of [REDACTED]

The McKinsey Project Manager for this effort: [REDACTED]

U.S. Customs and Border Protection points of contact:

Technical point of contact (POC):

Contracting Officer (CO):

Contracting Officer's Representative (COR):

Attachment(s):

1. Schedule of Supplies/Services
2. Accounting and Appropriation Data
3. Delivery Schedule
4. Statement of Work

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED

32b. SIGNATURE OF AUTHORIZED GOVT. REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

34. VOUCHER NUMBER

35. AMOUNT VERIFIED  
CORRECT FOR

36. PAYMENT

37. CHECK NUMBER

☐ PARTIAL ☐ FINAL

☐ COMPLETE ☐ PARTIAL ☐ FINAL

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

42a. RECEIVED BY (Print)

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42b. RECEIVED AT (Location)

42c. DATE REC'D (YY/MM/DD)

42d. TOTAL CONTAINERS

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: 70B01C18F00000497**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
20	Contract Support Services	1.000	AU		
30	Contract Support Services	1.000	AU		
40	Contract Support Services	1.000	AU		
50	Contract Support Services	1.000	AU		
60	Contract Support Services	1.000	AU		
70	Contract Support Services	1.000	AU		
80	Contract Support Services	1.000	AU		
90	Contract Support Services	1.000	AU		
100	Contract Support Services	1.000	AU		
110	Contract Support Services	1.000	AU		
120	Contract Support Services	1.000	AU		
130	Contract Support Services	1.000	AU		
140	Contract Support Services	1.000	AU		
150	Contract Support Services	1.000	AU		
160	Contract Support Services	1.000	AU		
170	Contract Support Services	1.000	AU		
180	Contract Support Services	1.000	AU		
190	Contract Support Services	1.000	AU		

**Total Funded Value of Award:**

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
20	6100.2525USCSGLCS0901010000Z00018500MA1100000000 970102525 TAS# 07020182018 0530000	
30	6100.2525USCSGLCS0901010000Z00018500AB0100000000 970102525 TAS# 07020182018 0530000	
40	6100.2525USCSGLCS0901010000Z00018500AB0200000000 970102525 TAS# 07020182018 0530000	
50	6100.2525USCSGLCS0901010000Z00018500AB0300000000 970102525 TAS# 07020182018 0530000	
60	6100.2525USCSGLCS0901010000Z00018500IP0100000000 970102525 TAS# 07020182018 0530000	
70	6100.2525USCSGLCS0901010000Z00018500IP0200000000 970102525 TAS# 07020182018 0530000	
80	6100.2525USCSGLCS0901010000Z00018500IP0300000000 970102525 TAS# 07020182018 0530000	
90	6100.2525USCSGLCS0901010000Z00018500IP0600000000 970102525 TAS# 07020182018 0530000	
100	6100.2525USCSGLCS0901010000Z00018500IP0700000000 970102525 TAS# 07020182018 0530000	
110	6100.2525USCSGLCS0901010000Z00018500IP0800000000 970102525 TAS# 07020182018 0530000	
120	6100.2525USCSGLCS0901010000Z00018500IP0900000000 970102525 TAS# 07020182018 0530000	
130	6100.2525USCSGLCS0901010000Z00018500MA1000000000 970102525 TAS# 07020182018 0530000	
140	6100.2525USCSGLCS0901010000Z00018500MA1100000000 970102525 TAS# 07020182018 0530000	
150	6100.2525USCSGLCS0901010000Z00018500MA1200000000 970102525	

	TAS# 07020182018 0530000	
160	6100.2525USCSGLCS0901010000Z00018500TT0100000000 970102525 TAS# 07020182018 0530000	
170	6100.2525USCSGLCS0901010000Z00018500TT0200000000 970102525 TAS# 07020182018 0530000	
180	6100.2525USCSGLCS0901010000Z00018500TT0400000000 970102525 TAS# 07020182018 0530000	
190	6100.2525USCSGLCS0901010000Z00018500TT0700000000 970102525 TAS# 07020182018 0530000	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 1300 Pennsylvania Av, NW Washington, DC 20229	20	1.000	07/15/2019
	30	1.000	07/15/2019
	40	1.000	07/15/2019
	50	1.000	07/15/2019
	60	1.000	07/15/2019
	70	1.000	07/15/2019
	80	1.000	07/15/2019
	90	1.000	07/15/2019
	100	1.000	07/15/2019
	110	1.000	07/15/2019
	120	1.000	07/15/2019
	130	1.000	07/15/2019
	140	1.000	07/15/2019
	150	1.000	07/15/2019
	160	1.000	07/15/2019
	170	1.000	07/15/2019
	180	1.000	07/15/2019
	190	1.000	07/15/2019

**I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)**

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

**I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)**



- (a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.
- (b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.
- (c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

**I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)**

**I.7 52.204-22 ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)**

**I.8 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)**

**I.9 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)**

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

**I.10 PERIOD OF PERFORMANCE (MAR 2003)**

The period of performance of this contract shall be from 07/16/2018 through 07/15/2019.

[End of Clause]

**I.11 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)**

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

**I.12 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)**

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

Task Order #

Work Authorization

- \_\_\_\_\_  
- \_\_\_\_\_  
- \_\_\_\_\_

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

#### **I.13 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)**

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

#### **I.14 SECURITY PROCEDURES (OCT 2009)**

##### **A. Controls**

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated

government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.

6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

#### B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2).
3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquiries, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).
4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

#### C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

**D. Notification of Contractor Employee Changes**

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.
2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

**E. Non-Disclosure Agreements**

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

**I.15 NON-PERSONAL SERVICE (MAR 2003)**

1. The Government and the contractor agree and understand the services to be performed under this contract are non-personal in nature. The Contractor shall not perform any inherently Governmental functions under this contract as described in Office of Federal Procurement Policy Letter 92-1
2. The services to be performed under this contract do not require the Contractor or his employees to exercise personal judgment and discretion on behalf of the Government, but rather, the Contractor's employees will act and exercise personal judgment and discretion on behalf of the Contractor.
3. The parties also recognize and agree that no employer-employee relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees. Contractor personnel under this contract shall not:
  - (a) Be placed in a position where there is an appearance that they are employed by the Government or are under the supervision, direction, or evaluation of any Government employee. All individual employee assignments any daily work direction shall be given by the applicable employee supervisor.
  - (b) Hold him or herself out to be a Government employee, agent or representative or state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as such and specify the name of the company of which they work.

- (c) Be placed in a position of command, supervision, administration or control over Government personnel or personnel of other Government contractors, or become a part of the government organization. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to change the contract in any way. If the other Contractor believes this communication to be direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.
- 4. If the Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the Contractor shall promptly notify the CO of this communication or action.
- 5. Rules, regulations directives and requirements which are issued by U.S. Customs & Border Protection under their responsibility for good order, administration and security are applicable to all personnel who enter U.S. Customs & Border Protection installations or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non-personal services contract.

[End of Clause]

#### **I.16 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2014)**

##### **A. Contractor Performance Evaluations**

Interim and final performance evaluation reports will be prepared on this contract or order in accordance with FAR Subpart 42.15. A final performance evaluation report will be prepared at the time the work under this contract or order is completed. In addition to the final performance evaluation report, an interim performance evaluation report will be prepared annually to coincide with the anniversary date of the contract or order.

Interim and final performance evaluation reports will be provided to the contractor via the Contractor Performance Assessment Reporting System (CPARS) after completion of the evaluation. The CPARS Assessing Official Representatives (AORs) will provide input for interim and final contractor performance evaluations. The AORs may be Contracting Officer's Representatives (CORs), project managers, and/or contract specialists. The CPARS Assessing Officials (AOs) are the contracting officers (CO) or contract specialists (CS) who will sign the evaluation report and forward it to the contractor representative via CPARS for comments.

The contractor representative is responsible for reviewing and commenting on proposed ratings and remarks for all evaluations forwarded by the AO. After review, the contractor representative will return the evaluation to the AO via CPARS.

The contractor representative will be given up to fourteen (14) days to submit written comments or a rebuttal statement. Within the first seven (7) calendar days of the comment period, the contractor representative may request a meeting with the AO to discuss the evaluation report. The AO may complete the evaluation without the contractor representative's comments if none are provided within the fourteen (14) day comment period. Any disagreement between the AO/CO and the contractor representative regarding the performance evaluation report will be referred to the Reviewing Official (RO) within the division/branch the AO is assigned. Once the RO completes the review, the evaluation is considered complete and the decision is final.

Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file and may be used in future award decisions.

##### **B. Designated Contractor Representative**

The contractor must identify a primary representative for this contract and provide the full name, title, phone number, email address, and business address to the CO within 30 days after award.

##### **C. Electronic Access to Contractor Performance Evaluations**

The AO will request CPARS user access for the contractor by forwarding the contractor's primary and alternate representatives' information to the CPARS Focal Point (FP).

The FP is responsible for CPARS access authorizations for Government and contractor personnel. The FP will set up the user accounts and will create system access to CPARS.

The CPARS application will send an automatic notification to users when CPARS access is granted. In addition, contractor representatives will receive an automated email from CPARS when an evaluation report has been completed.

(End of Clause)

#### **I.17 ADDITIONAL CONTRACTOR PERSONNEL REQUIREMENTS (OCT 2007)**

The Contractor will ensure that its employees will identify themselves as employees of their respective company while working on U.S. Customs & Border Protection (CBP) contracts. For example, contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.

The contractor will ensure that their personnel use the following format signature on all official e-mails generated by CBP computers:

[Name]  
 (Contractor)  
 [Position or Professional Title]  
 [Company Name]  
 Supporting the XXX Division/Office...  
 U.S. Customs & Border Protection  
 [Phone]  
 [FAX]  
 [Other contact information as desired]

[End of Clause]

#### **I.18 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)**

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
  - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
  - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.
  - c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

**I.19 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)**

- (a) **Applicability.** This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.
- (b) **Definitions.** As used in this clause—

*"Personally Identifiable Information (PII)"* means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

*"Sensitive Information"* is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

*"Sensitive Information Incident"* is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

*"Sensitive Personally Identifiable Information (SPII)"* is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an

individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

- (c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

- (d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

- (1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
- (2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.



- (3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
  - (4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.
- (e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.
- (1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.
    - (i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.
    - (ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.
    - (iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

- (2) **Renewal of ATO.** Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.
  - (3) **Security Review.** The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.
  - (4) **Continuous Monitoring.** All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.
  - (5) **Revocation of ATO.** In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.
  - (6) **Federal Reporting Requirements.** Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.
- (f) **Sensitive Information Incident Reporting Requirements.**
- (1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself,

be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

- (2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

- (1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
- (2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
- (3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
  - (i) Inspections,
  - (ii) Investigations,
  - (iii) Forensic reviews, and
  - (iv) Data analyses and processing.
- (4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

- (1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.
- (2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first

class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- (i) A brief description of the incident;
  - (ii) A description of the types of PII and SPII involved;
  - (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
  - (iv) Steps individuals may take to protect themselves;
  - (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
  - (vi) Information identifying who individuals may contact for additional information.
- (i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:
- (1) Provide notification to affected individuals as described above; and/or
  - (2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:
    - (i) Triple credit bureau monitoring;
    - (ii) Daily customer service;
    - (iii) Alerts provided to the individual for changes and fraud; and
    - (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
  - (3) Establish a dedicated call center. Call center services shall include:
    - (i) A dedicated telephone number to contact customer service within a fixed period;
    - (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
    - (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
    - (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
    - (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
    - (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.
- (j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of clause)

## **I.20 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)**

- (a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.
- (b) Security Training Requirements.
- (1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st

of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

- (2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.
- (c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

#### **I.21 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012)**

- (a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:
- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
  - (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
  - (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

- (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
- (b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
- (c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
- (d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
- (e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
- (f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

## **I.22 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012) ALTERNATE II (JUN 2006)**

- (a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:
  - (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
  - (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
  - (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
  - (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
- (b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

- (c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
- (d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
- (e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
- (f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.
- (g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.
- (h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non- U.S. citizens after contract award shall also be reported to the contracting officer.

(End of Clause)

## **SECTION III - STATEMENT OF WORK**

### **III.1 INTRODUCTION**

The United States (U.S.) Customs and Border Protection (CBP) is one of the Department of Homeland Security's (DHS) largest and most complex components with a priority mission of keeping terrorists and their weapons out of the U.S. CBP is the Nation's primary border security agency and its largest uniformed law enforcement organization. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws. CBP's mission covers a very broad spectrum of issues, from the apprehension of undocumented border crossers, to collection of almost \$50 billion in revenue for the U.S. Treasury.

### **III.2 SCOPE**

CBP requires assistance with development of a strategic assessment and with the development of strategic and tactical approaches required to position the agency to meet anticipated emerging and future challenges and requirements in furtherance of CBP's mission, "To safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel."

CBP intends to procure these services through a multiple award, hybrid (Firm Fixed Price or Labor Hour) Blanket Purchase Agreement (BPA). The BPA Holders shall provide comprehensive Integrated Consulting Services in accordance with requirements of this Section and the BPA Holders General Services Administration (GSA) Schedule under the Professional Services Schedule (PSS) 00CORP. Comprehensive services provided under this BPA are specifically for SIN 874 1 Integrated Consulting Services.

Consulting services shall be limited to those in support of the CBP Commissioner, Deputy Commissioner, and Agency Leadership Council initiatives or other important innovation efforts in furtherance of mission objectives. The BPA Holder shall ensure effective performance of all services described herein and shall tender for acceptance only those items that conform to the requirements of the BPA. The BPA Holder shall also be capable of handling multiple task orders simultaneously.

The BPA Holder shall have the knowledge and technical expertise in any subject matter related to integrated consulting solutions and services. The BPA Holder shall have the ability to write about a variety of topics along with having an understanding of the highly complex technical, legal, and social issues inherent to Government policy.

NOTE: The following services are not covered under this BPA:

- (a) Legal, expert witness, consulting, and audit services pertaining to financial matters
- (b) Consulting services relating to public relations



### **III.3 SPECIFIC BPA TASK ORDER TASKS**

The BPA Holder shall furnish all the necessary services, qualified personnel, material, equipment, and facilities not otherwise provided by the Government as needed to perform all services delineated in, and in accordance with BPA Task Order (TO) requirements within the scope referenced in Section III.2.

The BPA Holder shall provide expert advice and assistance in support of CBP's mission-oriented business functions within the scope of the applicable SINs. The following are examples of the types of integrated consulting services the BPA Holder may perform under this BPA. These examples are not all inclusive or restrictive in nature and do not constitute relief from exercising professional judgment in the performance of the integrated consulting services.

- (a) Management or strategy consulting, including research, change management, communication plans, evaluations, studies, analyses, scenarios/simulations, reports, business policy and regulation development assistance, strategy formulation on issues related to organization, operations, and business technology
- (b) Facilitation and related decision support services
- (c) Survey services, using a variety of methodologies, including survey planning, design, and development; survey administration; data validation and analysis; reporting, and stakeholder briefings
- (d) Advisory and assistance services in accordance with FAR 37.203
- (e) Mission-oriented business projects or programs and the achievement of mission performance goals.

Specific required tasks will be identified on each individual BPA TO.

### **III.4 TASK ORDER DELIVERABLES**

Deliverables will be described in each BPA TO issued under this contract. All deliverables are subject to review and approval by the ordering activity in accordance with inspection/acceptance procedures. The BPA Holder shall work with the BPA Contracting Officer (CO) to resolve any quality/requirement issues with these deliverables without additional cost.

### **III.5 BPA MANAGEMENT AND OVERSIGHT**

The BPA Holder shall identify a Program Manager (PM) to provide centralized administration of all orders placed under the BPA. The PM is required to correspond with the BPA Contracting Officer's Representative (COR).

The Government may require status reviews as frequent as on a monthly basis throughout the term of the BPA. Reviews shall be held as scheduled by the COR or the CO. During

these reviews, the BPA Holder shall report the status of BPA orders and any outstanding issues concerning the BPA.

The BPA Holder shall be available to engage in on-site meetings as required within a 24-hour notification within a 50 mile radius of Washington D.C. Time required to be available at any location beyond the 50 mile radius will be agreed upon the BPA CO and the BPA Holder.

### **III.5.1 BPA-Level Deliverables**

<b>ITEM</b>	<b>SOW REFERENCE</b>	<b>DELIVERABLE/EVENT</b>	<b>DUE DATE</b>
1	III.5	BPA Management and Oversight	Monthly (less if desired by the Government)
2	III.6	BPA Post Award Conference	Within 15 days after date of award

### **III.6 BPA POST AWARD CONFERENCE**

The BPA Holder shall attend a Post Award Conference (i.e., Kickoff Meeting) conducted by the BPA CO and other Government officials no later than 15 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the BPA CO, is to discuss technical and contracting objectives of the BPA and to discuss all requirements of the BPA. The Post Award Conference will be held at the Government's facility, located in the Washington, DC area.

### **III.7 CONTRACTOR PERSONNEL**

#### **III.7.1 Qualified Personnel**

The BPA Holder shall provide qualified personnel to perform all integrated consulting requirements specified in the SOW in accordance with the labor categories of the schedule. For T&M/LH type TOs, the BPA Holder shall certify on each invoice that all T&M/LH labor meets the minimum education and experience of each labor category specified in the schedule.

#### **III.7.2 Key Personnel**

The BPA Holder may designate specific senior level professional, technical and managerial personnel as key personnel who are essential to the successful performance of work under awarded BPA TOs. Key Personnel shall be identified in TO proposals, and shall be available for full-time assignment as necessary to efficiently manage and perform the work of the contract and shall be available on the effective date of TO award.

### **III.7.3 Program Manager**

The BPA Holder shall provide a PM who shall be responsible for all Contractor work performed under each awarded BPA TO. The PM shall be a single point of contact for the CO and the COR. It is anticipated that the PM shall be a senior level employee provided by the BPA Holder for this work effort. The PM is further designated as Key Personnel by the Government. Pursuant to HSAR 3052.215-70 Key Personnel of Facilities, the BPA Holder shall not replace the PM without prior acknowledgement and approval from the CO.

### **III.8 PLACE OF PERFORMANCE**

All work shall be performed at the BPA Holder's facility unless designated otherwise in each BPA TO. The Government anticipates the majority of support will be required in the Washington, D.C. metropolitan area, specifically CBP Headquarters located in Washington, DC. CBP will direct contractors to other CBP Facilities as required.

### **III.9 TRAVEL**

BPA Holder travel may be required to support the requirements of the BPA TO. Travel required by the Government outside the local commuting area(s) will be reimbursed to the BPA Holder in accordance with the Federal Travel Regulations (FTR). The BPA Holder shall be responsible for obtaining written approval from the BPA TO COR (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

The Government will not reimburse local travel within a 50-mile radius from the BPA Holder's primary place of performance. BPA Holder personnel may be required to travel to support the requirements of this contract and as stated on the delivery order. Travel performed for personal convenience or daily travel to and from work at the BPA Holder's facility or local Government facility (i.e., designated work site) shall not be reimbursed hereunder. Local parking in the Washington, D.C. metropolitan area is not covered by this SOW.

Allowable travel costs will be reimbursed, if incurred and approved by the COR prior to departure, for the cost of transportation, lodging, subsistence and incidental expenses in accordance with the FTR. The BPA Holder shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes, and cancellations under nonrefundable airline tickets are reimbursable as long as the changes are driven by the work requirement. Long distance travel may be required both in the Contiguous United States (CONUS) and Outside the Contiguous United States (OCONUS). The BPA Holder shall coordinate specific travel arrangements with the COR to obtain advance, written approval for the travel about to be conducted. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs.

### **III.10 PERIOD OF PERFORMANCE**

The BPA consists of a one-year base period and four (4) one-year option periods. The BPA Periods are as follows:

Base Period:	June 8, 2017 through June 7, 2018
Option Period 1:	June 8, 2018 through June 7, 2019
Option Period 2:	June 8, 2019 through June 7, 2020
Option Period 3:	June 8, 2020 through June 7, 2021
Option Period 4:	June 8, 2021 through June 7, 2022

### **III.11 GOVERNMENT INSPECTION AND ACCEPTANCE**

Inspection and acceptance of products and services shall be performed by a duly authorized Government representative identified in each BPA TO in accordance with the Inspection and Acceptance clauses in the GSA Schedule and as further defined in each BPA TO.

All deliverables will be inspected for content, completeness, accuracy and conformance to BPA TO requirements by the BPA TO COR or as detailed in individual order. The Government requires a period not to exceed thirty (30) calendar days after receipt of final deliverable items for inspection and acceptance or rejection unless otherwise specified in the BPA TO. Lack of timely Government response shall not be construed as Government acceptance of Contractor deliverables.

#### **Government Acceptance Period**

The COR will review deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying that the deliverable has been accepted.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted quotation. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

The COR will have five (5) business days to review deliverables and provide comments. The Contractor shall have three (3) business days to make corrections and resubmit deliverables. Lack of timely Government response shall not be construed as Government acceptance of Contractor deliverables.

All other review times and schedules for deliverables shall be agreed upon by the parties. The Contractor shall be responsible for timely delivery to Government personnel in the

agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

### **III.12 GOVERNMENT FURNISHED EQUIPMENT (GFE) AND INFORMATION (GFI)**

(a) The Government will furnish only that equipment necessary for the Contractor to carry out its work efforts under task order awards at the Government facility. This includes normal workspace accommodations such as desk, chair, desk phone, and computer. While performing work under task order awards in Government facilities, the Contractor may have the use of other normal office EIT devices, such as fax machines (not classified), copiers, projectors, etc. It is required that the contractor may have to obtain CBP Personal Identity Verification (PIV) cards as they are necessary to log into all computers and laptops.

(b) The Government will provide to the Contractor laptop, desktop or other portable devices upon the written consent of the COR justifying the need for such equipment.

(c) The Government will furnish all necessary related documentation in its possession that may be required for the Contractor to perform this contract.

# Statement of Work (SOW)

## *CBP STRATEGIC PLAN*

### 1. BACKGROUND:

United States (U.S.) Customs and Border Protection (CBP) is one of the Department of Homeland Security's (DHS) largest and most complex components with a priority mission of keeping terrorists and their weapons out of the U.S. CBP is the Nation's primary border security agency and largest uniformed law enforcement organization. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws. CBP's mission covers a very broad spectrum of issues, from the apprehension of undocumented border crossers, to collection of almost \$50 billion in revenue for the U.S. Treasury.

The extent of CBP's mission requires it to operate in locations across the globe, from attaches at U.S. Embassies and officers at preclearance locations overseas, to agents and officers at and between land, sea and air ports of entry across the United States.

To succeed in executing its mission, both today and in the future, CBP requires a strategy that serves as a guide for agency decisions and actions. Although CBP's Strategic Plan was written relatively recently in December of 2015, much has changed in our operating environment and in CBP leadership's vision for the future – the renewed emphasis on border security, the statutory requirements of trade enforcement, the opportunities provided by emerging technologies, the requirement to maintain and improve legacy IT infrastructure, and the challenges of recruiting, hiring and retaining agents and officers.

### 2. SCOPE:

This task order is required to procure integrated consulting services to develop a new Strategic Plan, ensuring the furtherance of the agency's mission objectives. CBP also requires the development of an approach to implement and communicate the strategic plan to make it relevant to its employees, stakeholders and partners.

### 3. APPLICABLE DOCUMENTS:

The Contractor's designated Project Manager shall be essential to the project's success and designated as Key Personnel. Key Personnel are subject to the conditions set forth in SECTION II – BPA TERMS AND CONDITIONS HSAR 3052.215-70 Key Personnel of Facilities (DEC 2003) in Base BPA #: TBD upon Award.

### 4. SPECIFIC TASKS:

**Task 1 – Conduct Project Kick Off Meeting.** The Contractor shall participate in a CBP kick-off meeting sponsored by CBP within two (2) business days of Task

Order award. The purpose of the meeting is to introduce key Government and Contractor personnel, review and discuss the anticipated project schedule, identify possible risks or issues, and to address any other issues the Government or Contractor wish to discuss. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable. The Contractor shall provide a written summary of the Project Kick-Off Meeting detailed in the meeting minutes.

Deliverables: (1) Project Kick-Off Meeting Minutes

**Task 2 – Review and Refine Strategic Objectives.** CBP recently defined a set of strategic objectives that will set the future direction of the agency:

- Achieve “One CBP” culture: All of CBP is working together to deliver the best of each Office to the mission, to our operational priorities, and to each other
- Attract and retain critical talent: CBP can hire, develop and retain the talent it needs to meet the demands of the mission today and the workforce needs of the future
- Accelerate technology deployment: IT systems are reliable and the workforce is equipped with the tools and innovations needed to meet emerging threats
- Deepen partnerships: Partnerships in the USG, across sectors, and around the world are expanded to strengthen shared intelligence and to anticipate, identify and address potential threats
- Enhance the stakeholder experience: Travelers, the trade community, and other stakeholders engage and interact with CBP in ways that meet or exceed their expectations.

Building on that list and accounting for the core missions of CBP – border security, trade and travel facilitation, and trade enforcement - this task will review the initial set of objectives for correctness, completeness, clarity and inclusion in the CBP Strategy.

Deliverable: (2) Final set of Strategic Objectives

**Task 3 - Define Strategic Choices.** Based on CBP's Strategic Objectives, develop a set of strategic choices that will drive how CBP can most effectively execute its mission - balancing risk, performance and cost across all of its mission spaces. This list may include consideration of areas to de-emphasize or entirely divest from.

Deliverable: (3) Final set of Strategic Choices

**Task 4 – Draft CBP Strategic Plan.** Using the deliverables from Tasks 2 and 3, draft a CBP Strategic Plan inclusive of the defined strategic objectives and strategic choices used to evaluate agency effectiveness and assist in better-informed management decisions.

Deliverable: (4) CBP Strategic Plan

**Task 5 – Develop Implementation Plan.** Develop an implementation plan to define a set of key initiatives that will enable CBP to meet the intent of its Strategic Objectives and a communications strategy that defines the most effective way to cascade the CBP Strategy (Task 4) to all CBP employees.

Deliverable: (5) Implementation Plan that includes:

- A list of Key Initiatives, to include (a) initiative owners, (b) a delivery roadmap that includes discrete actions to be performed by the owners, (c) a definition of success for each initiative, and (d) a method by which CBP leadership can track the outcomes for each initiative.
- A communications approach that defines the most effective way to cascade the strategy to all CBP employees. This approach will include a. developing high quality written briefing materials that can be presented to Congressional stakeholders and delivered to the entirety of CBP's workforce and b. drafting oral presentations and speeches for senior leadership to communicate the strategy to the workforce and external stakeholders.

**Task 6 – Meeting Facilitation.** Development of the CBP Strategy must include direction and feedback from CBP's most senior leaders. The contractor should conduct facilitated sessions over the course of the period of performance to gather data, provide information, and gain leadership consensus and approval.

Deliverable: (6) Facilitated Leadership sessions, as required

**Task 7– Reporting.** The Contractor shall provide progress updates in person or via conference call with CBP on a weekly basis. Progress Updates shall address schedule, performance and status of all deliverables to include activities that will affect the contract period of performance, problems/risks found, recommended solutions to problems/risks identified and work planned for the next period. At the COR's discretion, CBP may choose to receive progress updates less frequently if determined a meeting is unnecessary.

The Contractor shall provide a monthly project report in writing no later than the fifth of each month. Each report shall include a summary of all Contractor work performed under the contract, including, but not limited to, an assessment of technical status, schedule status, any travel conducted, and any Contractor concerns or recommendations from the previous month, a complete tracking of deliverable due dates and submission dates, upcoming action items, and risks identified during the weekly updates. This report shall be used to justify the billing for each reporting period.

The Contractor shall provide a draft Project Execution Plan to successfully complete all tasks outlined all task outlined in this SOW, within fifteen (15) days after award for CBP's review, comment and approval. The Contractor shall provide a final Project Plan to the COR not later than thirty (30) business days after TO award.

Deliverables:           (7) Weekly Update  
                              (8) Monthly Project Report



## (9) Project Execution Plan

### 4. PLACE OF PERFORMANCE:

Majority of the work will be completed at CBP facilities. The Contractor may be required to attend meetings at CBP Headquarters, Washington, DC; or an alternative site as specified by CBP.

### 5. PERIOD OF PERFORMANCE:

The Period of Performance (POP) in support of this Task Order is 12 months after date of award.